

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

--	--	--	--	--	--	--	--	--	--

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2018/2019

TEH3221 – ETHICAL HACKING AND SECURITY ASSESSMENT (All sections / Groups)

4 March 2019
2:30 PM – 4:30 PM
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 4 pages, including the cover page, with **FIVE** questions only.
2. Attempt all **FIVE** questions.
3. All questions carry equal marks and the distribution of the marks for each question is given.
4. Please write all your answers in the answer booklet provided.

Question 1

- (a) Compare **THREE** penetration testing methodologies. [6 marks]
- (b) Name and briefly explain **TWO** legal acts in Malaysia which are related to the action of accessing a personal computer without authorization. [4 marks]
- (c) Can we strengthen the security of TCP/IP protocol by encrypting the source and destination IP addresses in the TCP header? Justify your answer. [2 marks]

Question 2

- (a) Explain the following types of port scanning:
i. SYN scan
ii. Connect scan
iii. NULL scan
iv. XMAS scan
v. FIN scan [5 marks]
- (b) Explain **FOUR** prevention methods for the dumpster diving attack. [4 marks]
- (c) Explain the possible attack on the C code below which can force it to output You Win. Subsequently, suggest **ONE** solution for the attack.

```
#include<stdio.h>

int main(){
    int i=0;
    char str[4];

    printf("Enter 3 characters:\n");
    scanf("%s", str);

    if(i==0)
        printf("You Lose\n");

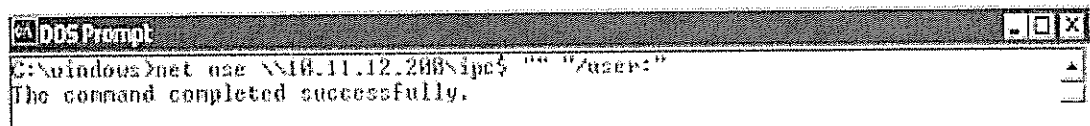
    else
        printf("You Win\n");
}
```

[3 marks]

Continued...

Question 3

- (a) The *Backdoor.Danton* trojan disguises itself as useful program through the port 6969. Describe the immediately steps to be taken when you discovered a PC is infected by this trojan, as well as the steps to remove it from the PC. [5 marks]
- (b) Refer to the following net command, answer the questions:



```

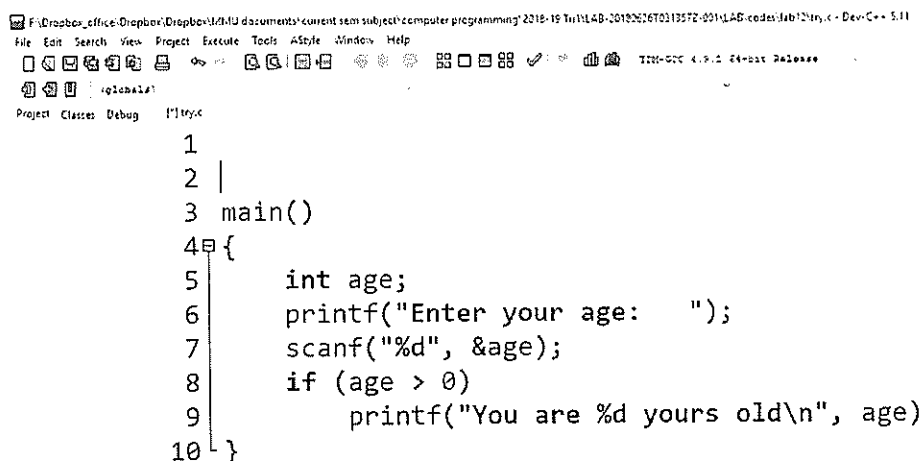
DOS Prompt
C:\windows>net use \\10.11.12.200\ipc$ "" /user:"
The command completed successfully.
  
```

This is a popular vulnerability within Windows, which can map an anonymous connection to a hidden share called IPC\$ which stands for interprocess communication.

- i. Briefly explain this hacking method. [2 marks]
- ii. What are the intentions that hackers launch this attack? Describe any **THREE** of the intentions. [3 marks]
- iii. What would you do to overcome this problem? [2 marks]

Question 4

- (a) Modify the C program below to eliminate the **TWO** errors in it.



```

1
2 |
3 main()
4 {
5     int age;
6     printf("Enter your age: ");
7     scanf("%d", &age);
8     if (age > 0)
9         printf("You are %d yours old\n", age)
10 }
  
```

[2 marks]

- (b) Explain Server Message Block (SMB) that is used for Windows. Provide **TWO** hacking tools which are able to cause damage to Windows networks. [4 marks]

Continued...

- (c) As a security professional, you are assigned to design a good password policy for your organization. Please provide any **THREE** statements that a password policy should include. [3 marks]
- (d) As a security professional, what principle should you advise your client organisation so that it is able to reduce the insider threats to them? [3 marks]

Question 5

- (a) *ABC* company is planting wireless network service in its corporate premise. The Information Technology (IT) department suggests to secure this wireless network by using WEP. What is WEP? Do you agree to the suggestion? Explain your answer. [3 marks]
- (b) If a company must use wireless technology, as a security professional, your job is to make it as secure as possible. Describe **FOUR** countermeasures for wireless attacks. [4 marks]
- (c) Explain about Symmetric Cryptography Algorithms. Devise **THREE** of its advantages. [5 marks]

End of page